National Weather Service

McAfee Endpoint Encryption for Files and Folders

Users Guide

December 2, 2010
Jeff Williams – Kristie O'Connor

Table of Contents

Why Endpoint Encryption for Files and Folders?

At a basic level most IT users are probably trusted to access their computers and use their documents, but at a higher level do you really want your system administrators to be able to read sensitive reports, personnel information, or other personal data?

Endpoint Encryption for Files and Folders allows NWS administrators to define data protection in a way that only certain users can read it. The encrypted data is stored as normal files; it can therefore still be managed, archived, and distributed but only understood by those who have been given proper access.

Endpoint Encryption for Files and Folders is a "Persistent Encryption" engine. Once you have encrypted a document, it's not possible to mistakenly create a decrypted copy of it. If you move a document out of an encrypted directory, it stays encrypted; if you move it to a removable device such as a memory stick, it remains encrypted.

Endpoint Encryption for Files and Folders also follows the Endpoint Encryption Policy control methods – NWS Administrators can set individual, office, FMC group, or NWS wide policies.

Design Philosophy

Endpoint Encryption for Files and Folders enhances the information security by providing data encryption and a strong authentication. You can use any login method, including passwords and Common Access Cards (when available) to access protected information.

The intent is to minimize user interaction related to information protection. Thus, the degree of user interaction is subject to policy control. It is possible for NWS Endpoint Encryption Administrators to set an environment where user's interaction is not required to do anything at all. The amount of user involvement is subject to encryption policies, which can be dynamically altered by your Endpoint Encryption Administrators as your security needs change.

How Endpoint Encryption for Files and Folders works

The Endpoint Encryption for Files and Folders client encrypts folders and documents according to policies set by NWS Endpoint Encryption Administrators, and delivered to you over the network. The Endpoint Encryption for Files and Folders client acts like a filter between the application creating or editing the information and the storage media, e.g. the hard disk.

The encryption/decryption happens automatically and is fully transparent. **You won't notice any difference between working with encrypted and plaintext documents; your working procedures are not, and must not, be disturbed.**

When a document is encrypted, it is encrypted at its original location on the disk. Hence, no copies or other special files are created when encrypting a document. The original document remains encrypted at all times, only the parts read into the memory are decrypted when an application, e.g. Microsoft® Word™, reads the document. When the application closes the document, the memory is wiped and the original document is still encrypted on disk. No decrypted traces of the document remain in the computer memory.

Endpoint Encryption for Files and Folders can encrypt documents and folders on basically all media platforms, whether it is the local hard disk, the file server or a USB flash memory.

Encrypted folders and documents are always visible to you if your key has been loaded. Thus, you can search for, and will recognize, documents and folders as they were before encryption. The only difference is a small padlock icon that can be optionally attached to the document or folder icon, marking it as encrypted.

With Endpoint Encryption for Files and Folders, it is easy to encrypt documents and folders. Encryption can be enforced either by a policy or by the user right-clicking folders and documents.

The document remains encrypted regardless of where it is moved. Thus, **the file will remain encrypted even if stored on a USB memory stick, a floppy disk or on a network share - persistent encryption**. This means that even if a document is misplaced in another folder, or placed on a floppy disk, it stays encrypted and always secure.

Documents moved to PDAs will lose their encryption. You will be presented a warning if moving encrypted documents to media not supported by Endpoint Encryption for Files and Folders. Documents moved from the PDA to an encrypted directory at the PC will certainly be encrypted

What encryption keys you can access is defined by your NWS Endpoint Encryption Administrator. You will receive your set of encryption keys when you have logged on to Endpoint Encryption. They are securely delivered to your Endpoint Encryption for Files and Folders client over the network. You must authenticate to Endpoint Encryption for Files and Folders before you can access the key, and thus access an encrypted document. The authentication is performed with the Endpoint Encryption logon dialog. Failing authentication renders you unable to read encrypted documents.

Endpoint Encryption for Files and Folders encrypts folders and documents transparently and on-the-fly, at the original location of the document or folder. Thus the amount of user interaction is very low and you will perceive your working environment almost as identical as before encryption.

As a user, you can never change or affect the policy that your Endpoint Encryption Administrator has applied to you. Your policy is enforced automatically in the background beyond your control. The reason for this is mainly to minimize the amount of extra work you need to do when working with encrypted data.

Endpoint Encryption for Files and Folders supports Endpoint Encryption FIPS 140-2 certified AES-256 algorithm.

With central management using the Endpoint Encryption Manager, and distribution of encryption keys using the secure Endpoint Encryption Server, it is easy to allow sharing of encrypted documents within an organization. When your NWS Endpoint Encryption Administrator assigns groups of users to encryption keys, the users in the group can exchange and read encrypted documents like any other document, without noticing any difference. Users not assigned to the key will not be able to read documents encrypted with that key.

Using this mechanism it is possible to protect documents and folders on shared units, e.g. a network server from unauthorized access by encrypting it with a proper key and allocating this key to authorized users only. This approach provides for encryption key hierarchies to be created, with an organization common key at the bottom (that every user has), to specific local office or group keys at the top (assigned only to selected users within that department or group).

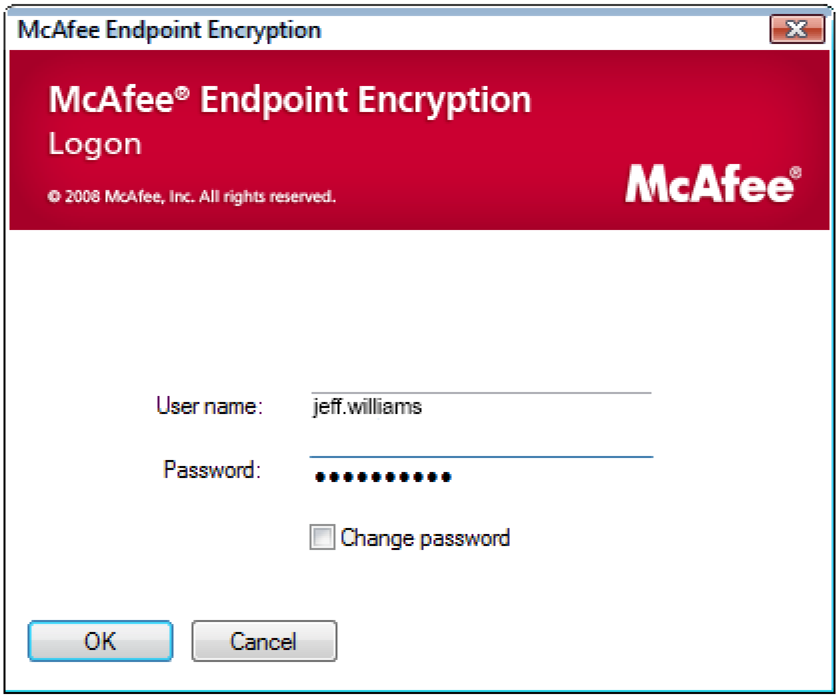
Management

When you authenticate to Endpoint Encryption for Files and Folders, the software communicates with an Endpoint Encryption Server to update its policy and Folders, i.e. try to access encrypted documents or do a manual Endpoint Encryption for Files and Folders logon, provided that you are online. Endpoint Encryption for Files and Folders will work also when offline, provided that the NWS Endpoint Encryption Administrator has made the central encryption key(s) available for offline use.

The Endpoint Encryption Administrator creates policies that are applied to you. Whenever you logon, your policy is applied and updated. Your Endpoint Encryption Administrator may also force you to do an initial logon after the client has been installed on your computer. You will notice such a forced logon in that you cannot close the authentication window before you have authenticated.

Endpoint Encryption for Files and Folders client

When you try to access encrypted documents, Endpoint Encryption for Files and Folders automatically recognizes this and prompts you to authenticate. If successful, the document data is transparently decrypted and the appropriate application started.



McAfee Endpoint Encryption

McAfee® Endpoint Encryption

Logon

© 2008 McAfee, Inc. All rights reserved.

User name: jeff.williams

Password: ●●●●●●●●●●●

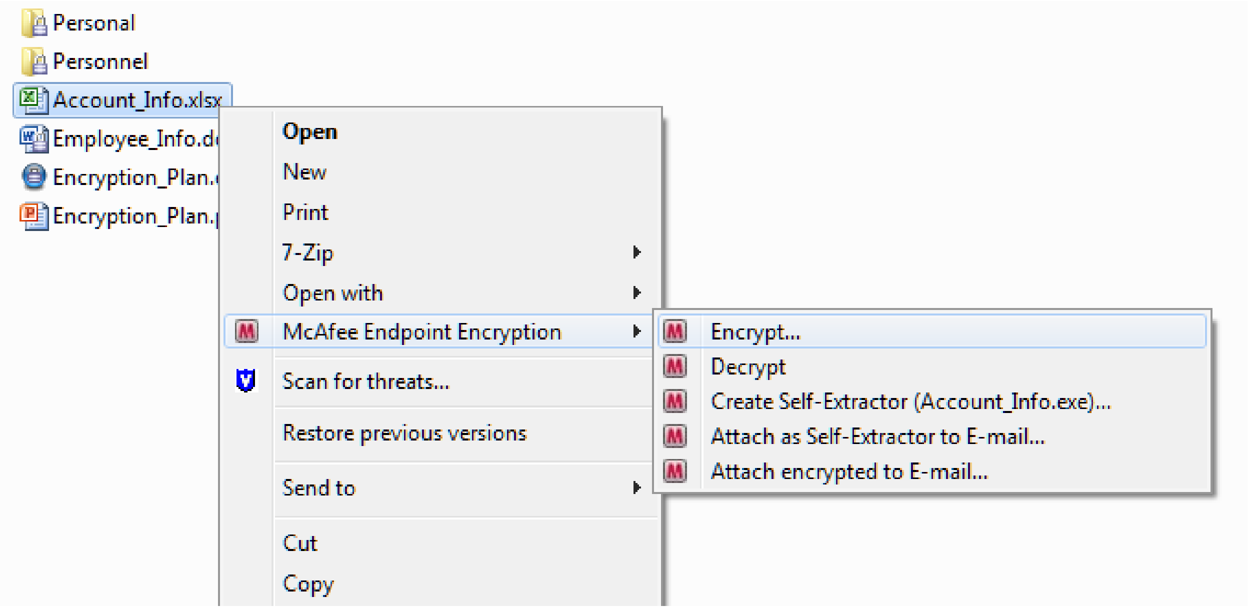
□ Change password

Endpoint Encryption for Files and Folders authentication dialog

The Context Menu Options (right-click menu options)

This section will deal with the options that are available when you right-click a document or folder, i.e. the context menu options. Since the context menus for folders and documents are almost identical as far as Endpoint Encryption for Files and Folders is concerned, they are described here in common. Any differences in behavior between a folder context menu option and the same option in the document context menu will be described accordingly.

Each of the context menu options are subject to policy control and may be made unavailable to you by your NWS Endpoint Encryption Administrator. When right-clicking document and folders you will see the entry *McAfee Endpoint Encryption,* which in turn has a submenu containing the options your Administrator has enabled for you.

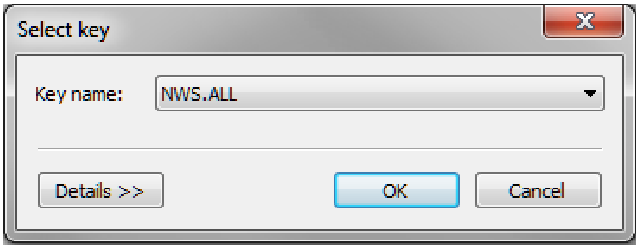

Personal
Personnel
Account_Info.xlsx
Employee_Info.d
Encryption_Plan.
Encryption_Plan.
Open
New
Print
7-Zip
Open with
McAfee Endpoint Encryption
Scan for threats...
Restore previous versions
Send to
Cut
Copy
Encrypt...
Decrypt
Create Self-Extractor (Account_Info.exe)...
Attach as Self-Extractor to E-mail...
Attach encrypted to E-mail...

Context menu when right-clicking a document (file)

Encrypt...

This option allows you to manually encrypt a file (document) or folder. If your Endpoint Encryption administrator has already set an encryption policy for a particular file or folder, this option will be "grayed out" in the context menu, i.e. you cannot select the option for that particular file or folder as it is already encrypted by a centrally defined policy.

When selected (if enabled and active), the option opens up an encryption dialog where you can make a key selection.



Key name: NWS.ALL

Endpoint Encryption for Files and Folders– Encrypt options

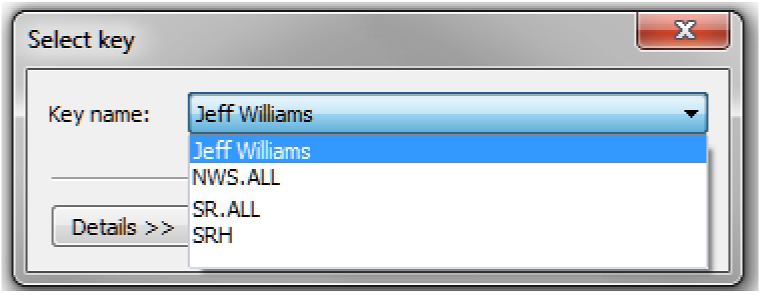
You may change the following:

Select key

You can select what encryption key to use from a drop-down menu. Standard keys that will be available to all users are:

NWS.ALL	All NWS users
XX.ALL (XX = FMC)	All FMC users
YYY (YYY= Office ID)	All local office users

Optionally, Administrators can set up keys for specific users and groups as necessary. If utilized, user keys will be created with the following naming standard of Firstname.Lastname.



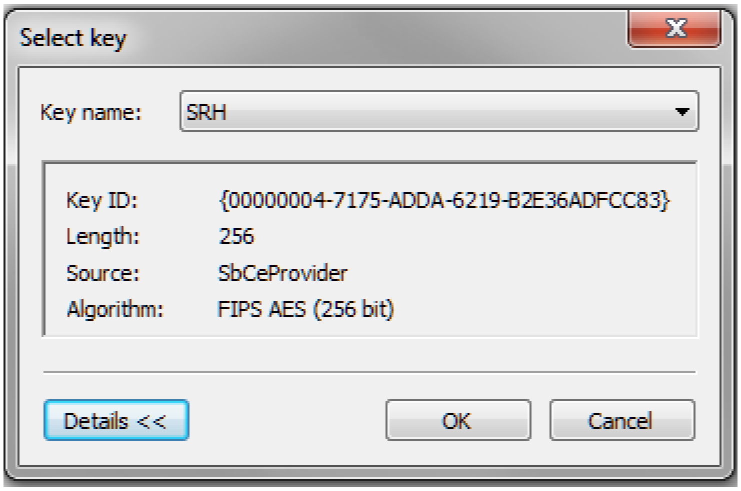
Key name: Jeff Williams

Details >>

This button opens up a dialog displaying additional information about the selected encryption key.

When you have selected your encryption key, click **OK** to launch the encryption, you may be asked to authenticate if the encryption key selected is not present.

Depending on the amount of data to encrypt, there may be a bar stating the progress of the encryption. At the end of the encryption, a dialog is presented telling the result of the encryption. In some cases, the product may fail to encrypt some documents in a folder. Most typically, this is because the document is opened by another application. For example, if encrypting a text document while having the document open for editing, the encryption will fail. The application must first be closed and then re-encrypting the document using the right-click operation.



Key name: SRH

Key ID: {00000004-7175-ADDA-6219-B2E36ADFCC83}
Length: 256
Source: SbCeProvider
Algorithm: FIPS AES (256 bit)

Endpoint Encryption for Files and Folders– Encrypt options- Details

Decrypt…

This option allows you to manually decrypt a file (document) or folder. If your Endpoint Encryption administrator has already set an encryption policy for a particular file or folder, this option will be "grayed out" in the context menu, i.e. you cannot select the option for that particular file or folder as it is already encrypted by a centrally defined policy and you cannot change the encryption status.

When selected (if enabled and active), the option directly decrypts the selected file and folder.

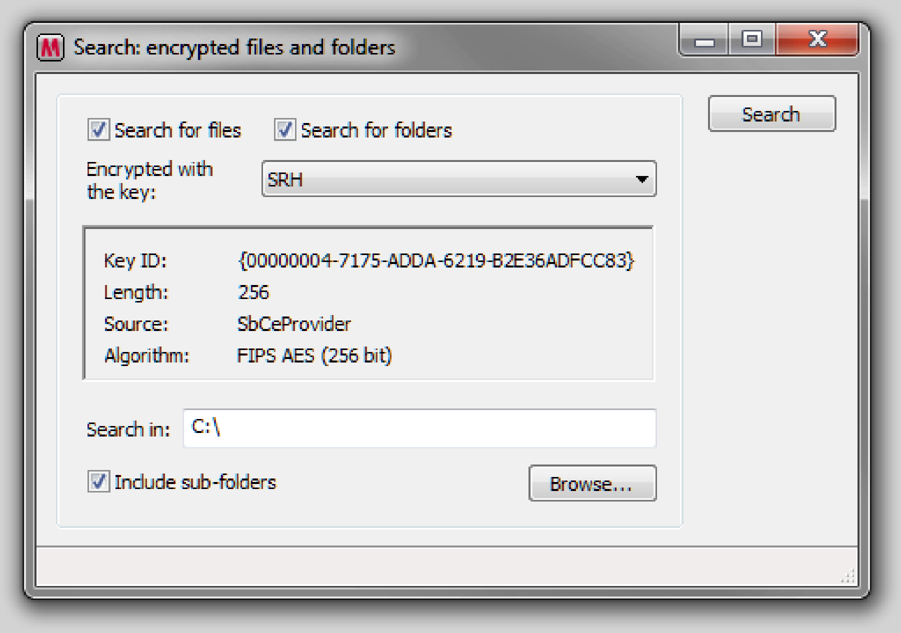
For both file decryption and folder decryption you may be asked to authenticate if the encryption key needed for the decryption is not present.

Again, the decryption happens immediately (without any intermediate dialog) provided the user has proper rights to do so.

Depending on the amount of data to decrypt, there may be a bar stating the progress of the decryption. At the end of the decryption, a dialog is presented telling the result of the decryption. In some cases, the product may fail to decrypt some documents in a folder. Most typically, this is because the document is opened by another application. For example, if encrypting a text document while having the document open for editing, the decryption will fail. The application must first be closed and then re-decrypting the document using the right-click operation.

Search encrypted... (Folder context menu only)

This function allows you to search for encrypted documents and folders on the location you specify. This option is only available when right-clicking a folder, or the Windows **Start** button. When selected, a search dialog opens up that allows you to specify the details of the search.



Search: encrypted files and folders

☑ Search for files ☑ Search for folders

Encrypted with the key: SRH

Key ID: {00000004-7175-ADDA-6219-B2E36ADFCC83}
Length: 256
Source: SbCeProvider
Algorithm: FIPS AES (256 bit)

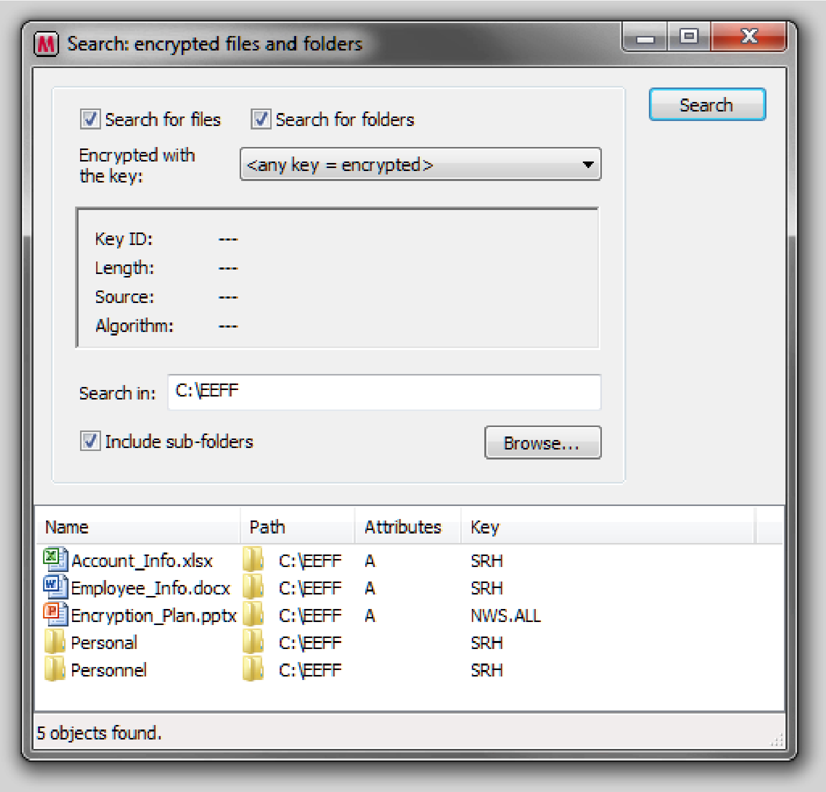
Search in: C:\

☑ Include sub-folders

Endpoint Encryption for Files and Folders– Search dialog

Specify the parameters for the search, e.g. search for all files (documents) and folders encrypted with a particular key (or <any key>) on this location. You may also select to search for encrypted files only, encrypted folders only or both. At the bottom, you may also select if you want to include all subfolders in the search. Enter the location for the search start, either by typing in the correct location or by clicking the **Browse…** button.

When ready, click Search to launch the search. As the search progresses, matching objects found will be displayed in a list.



☑ Search for files ☑ Search for folders

Encrypted with the key: <any key = encrypted>

Key ID: ---
Length: ---
Source: ---
Algorithm: ---

Search in: C:\EEFF

☑ Include sub-folders

Name	Path	Attributes	Key
Account_Info.xlsx	C:\EEFF	A	SRH
Employee_Info.docx	C:\EEFF	A	SRH
Encryption_Plan.pptx	C:\EEFF	A	NWS.ALL
Personal	C:\EEFF		SRH
Personnel	C:\EEFF		SRH

5 objects found.

Endpoint Encryption for Files and Folders– Search Results

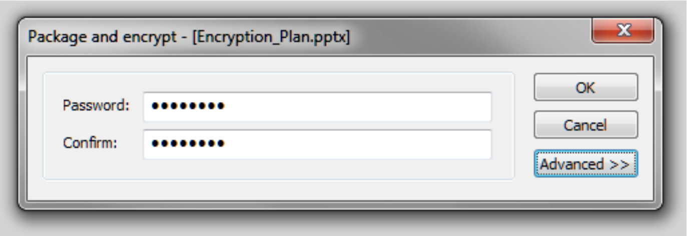
Once the search is complete, the objects found may be marked with "Ctrl-A" and then any action can be performed on them, e.g. right-click and select **Decrypt**.

Create Self-Extractor ({filename}.exe)…

This option allows you to create so-called Self-Extractors. A Self-Extractor is a special package that is encrypted with a selected password only and can be read on any computer without installing any programs. There is no need to have Endpoint Encryption for Files and Folders installed in order to read a Self-Extractor. Only the password used to create the Self-Extractor is needed in order to unpack and read it.

When you select this option a Self-Extractor is created of whatever file (document) or folder you choose to do the operation on. Note that the source file/folder will remain intact on disk, only a copy of the file/folder is converted into a Self-Extractor.

Once the menu option is selected, you are asked to provide the password to create the Self-Extractor:



Package and encrypt - [Encryption_Plan.pptx]

Password: ••••••••

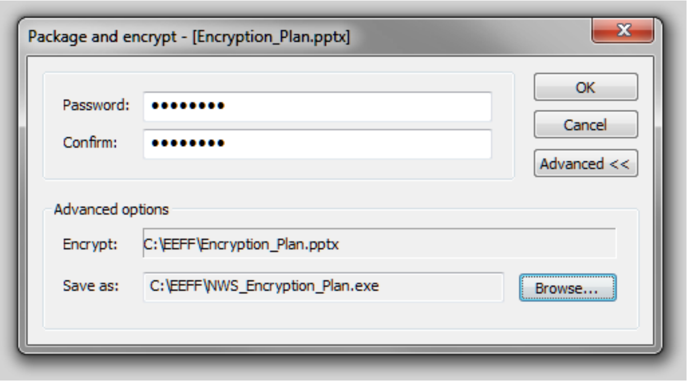
Confirm: ••••••••

Entering encryption password for self-extracting file

You need to enter the special password that the Self-Extractor will be encrypted with. You may also specify where to save the Self-Extractor. The default location is the same as the location of the source file/folder. Also, you may change the name of the Self-Extractor. By default, it is named as its source file/folder with the *.exe extension.

NOTE: The same password rules apply for the Self-Extractors as for your normal Endpoint Encryption password. For example, if you have a minimum password length of 12 characters for your Endpoint Encryption password, the minimum password length for the Self-Extractor is also 12 characters.

By clicking advanced, you may specify where to save the Self-Extractor once created.



Package and encrypt - [Encryption_Plan.pptx]

Password: ••••••••

Confirm: ••••••••

Advanced options

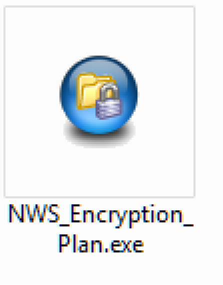
Encrypt: C:\EEFF\Encryption_Plan.pptx

Save as: C:\EEFF\NWS_Encryption_Plan.exe

Specifying the location for the Self-Extractor

If you like, you may browse for a suitable storage location, e.g. a USB memory stick attached to the computer, by clicking **Browse**.

When finished, click **OK,** and the Self-Extractor is created. The Self-Extractor file has the following icon:



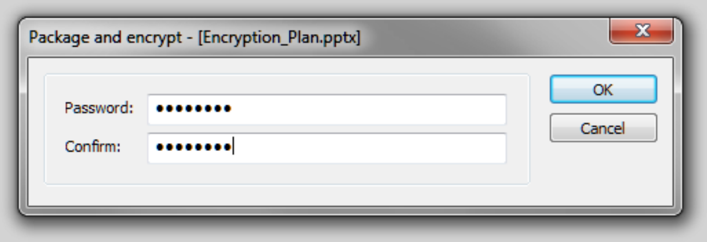
Example of Self-Extractor

Attach as Self-Extractor to E-mail...

When selecting this option, the Self-Extractor is automatically packaged into a format suited for e-mails (*.cab) and attached to a new e-mail. Any e-mail program can be used for this.

Even if the *.cab file gets through in your e-mails, it may happen that e-mails sent with a *.cab Self-Extractor attachment are blocked by the recipients anti-virus program.

Before you can create the Self-Extractor as an attachment, you are asked to provide a password to be used to encrypt the Self-Extractor.


Package and encrypt - [Encryption_Plan.pptx]

Password: ••••••••

Confirm: ••••••••

Entering encryption password for Self-Extractor to e-mail attachment

By clicking **OK**, the attachment is created in a new e-mail ready to be sent.

Attach encrypted to E-mail... (Files only)

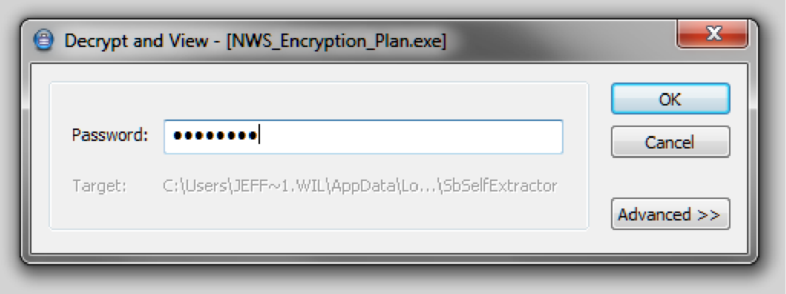
This option allows you to send a particular document (plaintext or encrypted) in a protected way to a colleague that also has Endpoint Encryption installed. The option creates a special encrypted format of the document and attaches it automatically to an e-mail that you can send. The recipient must have Endpoint Encryption for Files and Folders installed and also have access to the encryption key used when creating the encrypted attachment.

NOTE: If you attach an encrypted document to an e-mail without using the Attach encrypted to E-mail... function, the document will remain encrypted if using Thunderbird or Outlook by NWS Endpoint Encryption Policy. If a program other than Thunderbird or Outlook are used the document will be attached in plaintext even if the document is encrypted on disk. The source document will still be

encrypted though, but the copy created as attachment will be in plaintext and the recipient will receive it in plaintext.

Reading a Self-Extractor File

To read a Self-Extractor you simply double-click the Self-Extractor. You will be prompted for the special password used to create the Self-Extractor. Thus, the creator of this file must submit the password to the recipient of the file in a secure manner.



Decrypt and View - [NWS_Encryption_Plan.exe]

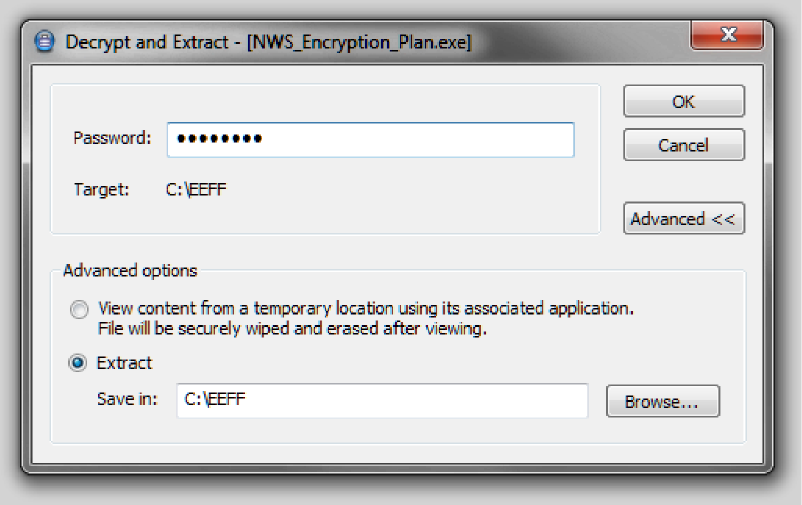
Password: ••••••••

Target: C:\Users\JEFF~1.WIL\AppData\Lo...\SbSelfExtractor

Opening (decrypting) a Self-Extractor

By default, after typing the correct password the content of the Self-Extractor will open up automatically in the associated application However, the **content won't be automatically saved to disk**. When the user closes the application that opened up the unpacked Self-Extractor content, the unpacked content will be wiped from the disk. If the user instead wants to save the Self-Extractor content to disk, the **Advanced >>** button must be selected.

This opens up an extra dialog where the user may select what to do with the unpacked and decrypted Self-Extractor.



Decrypt and Extract - [NWS_Encryption_Plan.exe]

Password: ••••••••

Target: C:\EEFF

Advanced options

○ View content from a temporary location using its associated application. File will be securely wiped and erased after viewing.

● Extract

Save in: C:\EEFF

Selecting what to do with the content of the Self-Extractor

Self-Extractors may be read on any computer running Windows 2000 and later. There is no need to have the Endpoint Encryption for Files and Folders client installed. Nor is there any need to have local administrator rights in order to open a Self-Extractor.

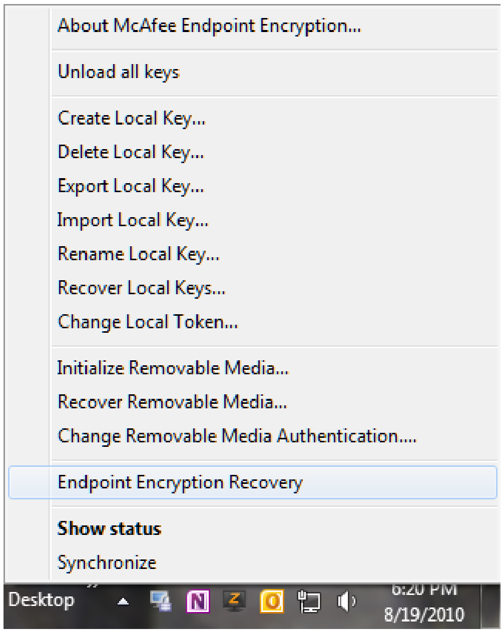
By default, the **open-close-wipe** option is selected. If the **Extract** option is selected instead, the user may select where to permanently save the unpacked and decrypted Self-Extractor. The user may browse for a suitable location with the **Browse** button.

The tray icon options

This section deals with the options that are available from the Endpoint Encryption product tray icon menu. When you have had Endpoint Encryption installed on your computer, you will see a new icon in your system tray, i.e. the bar of icons typically located at the bottom right corner of your screen. The Endpoint Encryption tray icon is common for all Endpoint Encryption products installed and it looks as follows (a computer with a gray padlock attached to it):

The Endpoint Encryption product tray icon

Depending on how many Endpoint Encryption products you have installed, the content of the menu when you right-click this icon will differ. The below image shows the menu when only Endpoint Encryption for Files and Folders is installed.



Endpoint Encryption for Files and Folders tray icon menu options

Some of these options may not be visible to you. This means that they have been disabled for you in your encryption policy by your Endpoint Encryption

Administrator. Each of the menu options is described below.

About Endpoint Encryption for Files and Folders

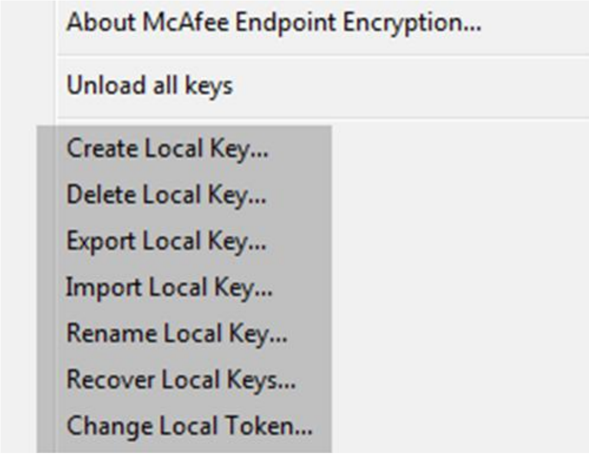
This dialog opens up a window that contains a description of your installation of Endpoint Encryption for Files and Folders. Typically, there is no need for the regular user to get acquainted with the content of the **About…** window. Should you have any questions about this option, please contact your Endpoint Encryption Administrator.

Unload all keys

Selecting this option effectively closes all encryption keys that are available to your system. This means that you need to authenticate again before you can access encrypted data, i.e. you need to open the keys for use again. It is good security practice to close all keys before you leave your computer unattended for a period of time. However, there are also other security parameters in Endpoint Encryption for Files and Folders that the NWS Endpoint Encryption Administrator may have enabled for automatic key closing. Ask your Endpoint Encryption Administrator about proper use of this manual option.

User Local Key management options (If available in Policy)

If your NWS Endpoint Encryption Administrator has enabled the Local Key option you will find the following options to manage your local keys. **(See section below for a more detailed explanation on local key management.)**



Endpoint Encryption for Files and Folders user local key management options

Endpoint Encryption Recovery

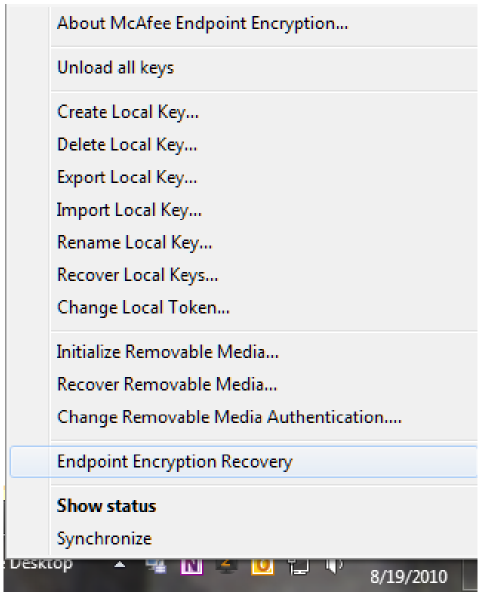
This option starts the recovery process, should you have forgotten your Endpoint Encryption password. Follow the wizard that starts when you select this option. The recovery process requires interaction with the Endpoint Encryption central database.

You don't need to be online in order to do a recovery. Recovery will work even if you have no contact with any network.

The explanation below assumes a verbal interaction with your NWS Administrator; the web recovery approach is very similar.

1. Call your NWS Endpoint Encryption Administrator.

2. Start the recovery wizard from you tray icon menu



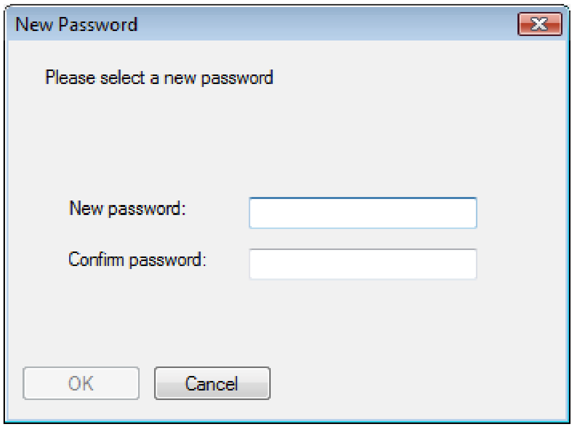
Recovery start from tray icon menu

3. Enter your Endpoint Encryption user name and click **Next >**.

4. Read out the challenge code to your Administrator, **click Next >.**

5. Enter the response codes that your Administrator reads out to you, after each line click **Enter**. If you mistype a code, you will be notified about this.

6. After entering the last code, click **Next >** and you will then be asked to enter a new password. Note that you still need to comply with the password quality rules.



Selection of new password after completed recovery

7. Once you have selected a new password, click **OK** to proceed and finish the recovery. Click **OK** to close the confirmation dialog and then **Finish** to complete the recovery. You can use the new password immediately to logon to Endpoint Encryption.

Show status

This option opens a dialog presenting the ongoing activities in the Endpoint Encryption for Files and Folders client. For example, if the client is active in encrypting the content of a network folder, it will be displayed in the dialog along with an approximation for how long it will last.

There are also two buttons available:

Diagnostics

This button automatically creates an e-mail with an attachment using the system default e-mail application. The attachment contains non-sensitive information for support purposes. The better description of the machine needing support, the better understanding the support staff will get and thus the chance of a quick resolution of the support issue is improved.

The e-mail with the attachment shall be sent to your station Endpoint Encryption administrator along with a description of the support issue.

Again, it is important to stress that no secret or sensitive information is collected. Under no circumstances is sensitive information about encryption keys included, nor are any encryption keys, or pieces of these, ever included. As you may verify by reviewing the attachment in a standard Web browser, there is no data disclosure of documents stored on the computer.

Synchronize

This button triggers client synchronization with the Endpoint Encryption central system. See next section for details.

Synchronization

Synchronizing Endpoint Encryption for Files and Folders triggers an authentication to the central Endpoint Encryption system. During synchronization, your policy is updated to reflect any changes in the Endpoint Encryption central system. Also, all encryption key assignments and settings are updated.

Also, any successful Endpoint Encryption for Files and Folders authentication, when online with the central system, automatically updates your policy and the encryption key settings. Hence, it is not necessary to do a manual Synchronization to get the policy updated; yet the option exists for immediate synchronizations.

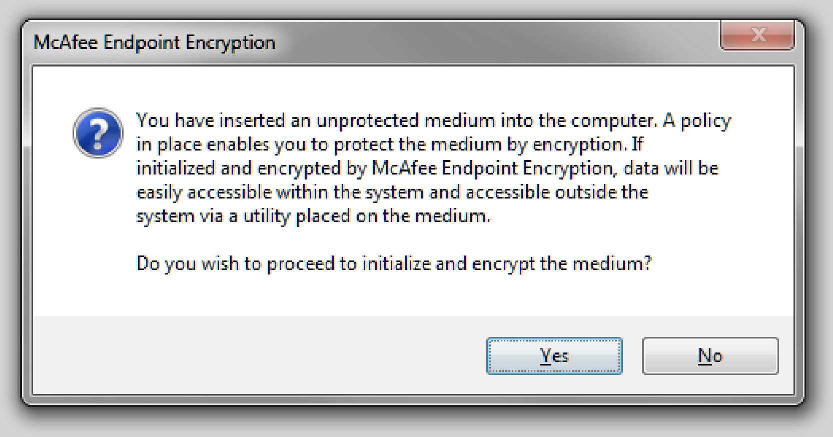
Endpoint Encryption for Removable Media (EERM)

What is McAfee EERM?

McAfee Endpoint Encryption for Removable Media (EERM) is a software solution that protects removable devices; primarily, USB thumb drives commonly referred to as “memory sticks”. However, any attached removable storage can be protected with EERM.

User experience

When you insert a non-protected removable device on a client with Endpoint Encryption for Files and Folders (EEFF) installed and the policy for removable media encryption states “EERM protection”, the following happens: A notification will be displayed telling you that you have inserted an unprotected medium into the computer.


McAfee Endpoint Encryption

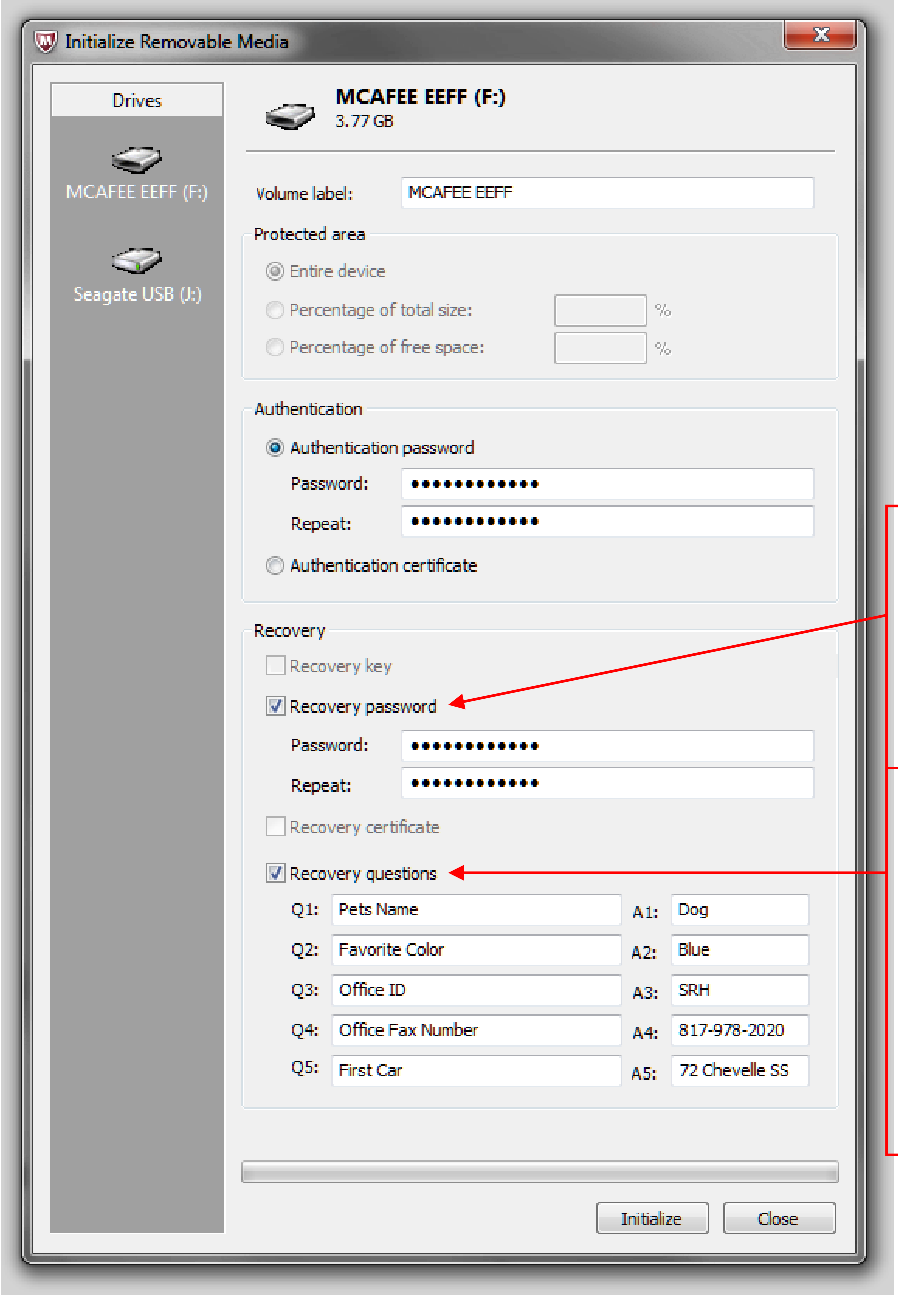
You have inserted an unprotected medium into the computer. A policy in place enables you to protect the medium by encryption. If initialized and encrypted by McAfee Endpoint Encryption, data will be easily accessible within the system and accessible outside the system via a utility placed on the medium.

Do you wish to proceed to initialize and encrypt the medium?

Notification dialog

The initialization of the device starts with a notification dialog. You can choose to protect the media, or ignore it with **Yes** and **No,** respectively. If you select "**Yes**" the initialization of the device with EERM will start according to what the policy specifies.

NOTE: Currently if you click **No**, the media will be writable while inserted. This setting will probably change in the future as NWS policy is developed for USB devices and if **No** is selected the drive will not be writable.



MCAFEE EEFF (F:)
3.77 GB

Volume label: MCAFEE EEFF

Protected area

● Entire device

○ Percentage of total size: %

○ Percentage of free space: %

Authentication

● Authentication password

Password: ••••••••••••

Repeat: ••••••••••••

○ Authentication certificate

Recovery

□ Recovery key

☑ Recovery password

Password: ••••••••••••

Repeat: ••••••••••••

□ Recovery certificate

☑ Recovery questions

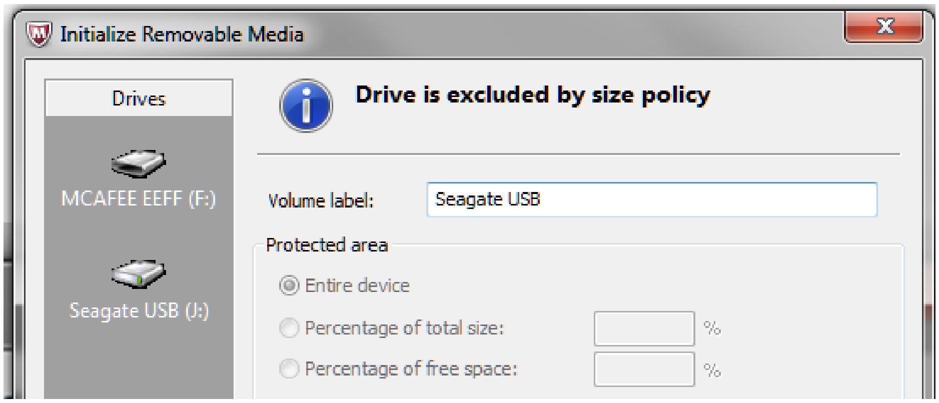
Q1:	Pets Name	A1:	Dog
Q2:	Favorite Color	A2:	Blue
Q3:	Office ID	A3:	SRH
Q4:	Office Fax Number	A4:	817-978-2020
Q5:	First Car	A5:	72 Chevelle SS

If selected, the user will need to provide a password that can be used for recovery.

If selected, the user will need to provide the question and answers. During recovery the answers must be typed **exactly** as entered during the initialization.

Initialization dialog

Note: If you also have a drive larger than 64GB such as an external disk you will not be able to encrypt the drive due to the current EERM policy. This is currently set to protect users from accidentally encrypting large drives. The policy may change as users become familiar with EERM or requirements change to protect larger drives.



Initialize Removable Media

Drives: MCAFEE EEFF (F:), Seagate USB (J:)

Drive is excluded by size policy

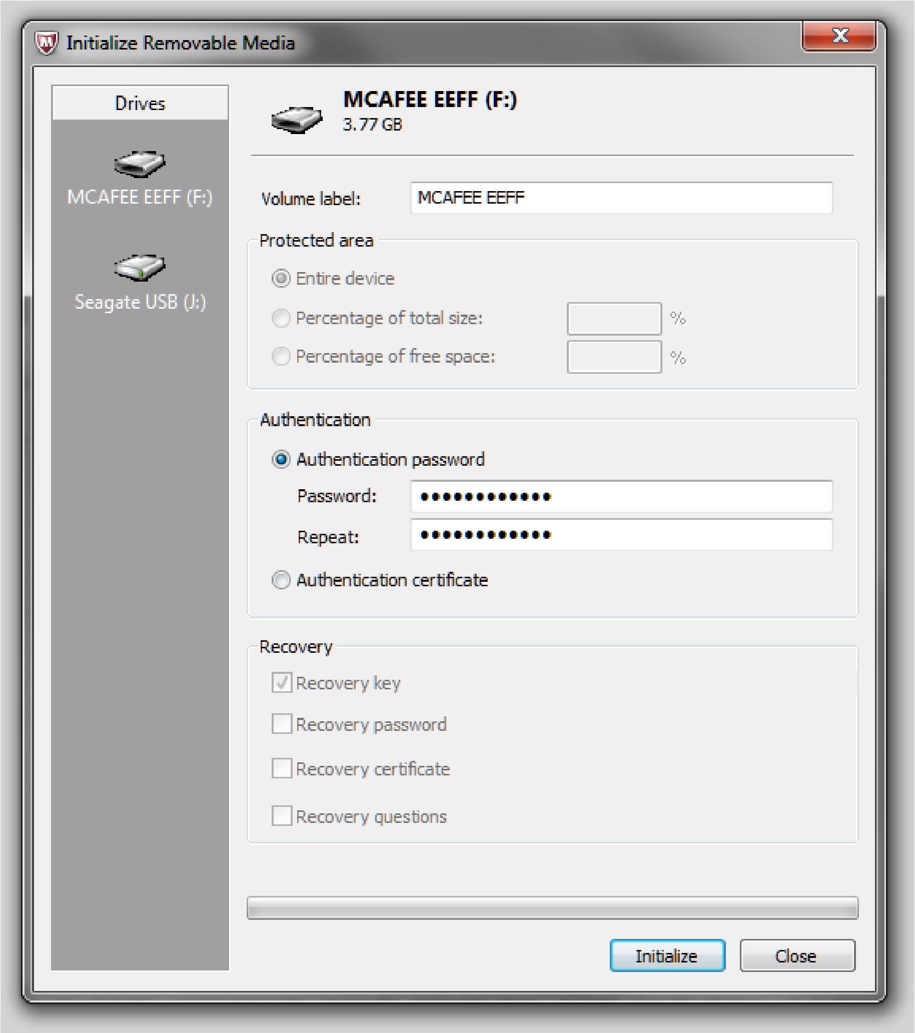
Volume label: Seagate USB

Protected area

- ● Entire device
- ○ Percentage of total size: %
- ○ Percentage of free space: %

Initialization dialog for drive excluded by policy

If you select to protect the media, an initialization dialog will be presented where the content will depend on what is set in your encryption policy. Fill out the information requested in the dialog in order to finish the initialization.



Initialize Removable Media

Drives: MCAFEE EEFF (F:), Seagate USB (J:)

MCAFEE EEFF (F:)
3.77 GB

Volume label: MCAFEE EEFF

Protected area

- ● Entire device
- ○ Percentage of total size: %
- ○ Percentage of free space: %

Authentication

- ● Authentication password
  - Password: ••••••••••••
  - Repeat: ••••••••••••
- ○ Authentication certificate

Recovery

- ☑ Recovery key
- □ Recovery password
- □ Recovery certificate
- □ Recovery questions

Initialization dialog

The fields that can be filled in are:

Authentication

In this section you shall enter the authentication method. Here you will enter a password for the encrypted device. The password policy will follow the password policy of the machine running EERM. This should match the DOC/NOAA/NWS policy of 12 characters.

The selection fields cannot be left empty, i.e. you must fill in valid authentication credentials.

Recovery

The default policy set up by the NWS Endpoint Encryption Administrators is set to use password and/or recovery questions for recovery.

Recovery questions

When marking this checkbox, you can enter five questions and answers that will be used in a recovery situation. I.e. you will be able to recover the encrypted device by again answering the selected questions without any interaction with your Administrator. Also, you can do this recovery from a computer without the EEFF client installed.

Note: It is sufficient for you to answer four out of five questions correct. Four correct answers will allow the recovery to succeed.

Initialize

When you have done all the selections in the initialization dialog, clicking the **Initialize** button will launch the initialization of the device as per the policy and your input.

The progress of the initialization is displayed in the progress bar at the bottom of the dialog. It is strongly recommended not to unplug the device during initialization or to cancel the initialization process. This may result in a device in “unknown state”, i.e. it cannot be used on a machine with EEFF installed.

Initialization complete and Authentication

Once the initialization is complete, an authentication dialog may appear requesting the user to authenticate to the device. If such a dialog appears, simply fill in the authentication information and then start working with your device.

Note: If there has been a failing initialization operation previously on the system, a message will state that a few files needs to be wiped from the system used during the initialization. Simply click **Yes** to do this operation.

Once initialized, the device can be used on any (Windows) machine without requiring any software installation.

Note: If the device has entered an "unknown state" as a result of you unplugging the device during initialization or canceling the initialization, the device can be formatted from a system without EEFF installed, using standard Windows format. After that, the device can again be protected with EERM.

A device encrypted with EERM is not protected against re-formatting from other systems where EEFF is not installed. You can re-format an EERM protected device on such machines, but do remember that such an operation will erase everything on the device, including all your files. When you again try to use that device on a system with EEFF installed and EERM protection enabled, you will be asked to re-protect your device. You will then need to enter all recovery information and password(s) again.

Working with device – "Online"

After successful initialization of the device, you will be promoted to authenticate when the drive is inserted into a machine running Endpoint Encryption for Files and Folders. If the machine does not have the EEFF installed you will need to navigate to the root of the USB device and run the **MFEeerm.EXE** program for authentication manually if auto run is disabled on the system

If you have forgotten your password or lost your certificate, you can click **Recover…**. The recovery process is described later in this guide.

If you enter a wrong password three consecutive times, the authentication dialog will offer the option to do a recovery. You may click **Yes**, in which the recovery dialog starts, or **No** in which case you will need to restart the authentication.

Once authenticated, you will see the encrypted folder as a drive in the system. Encrypted items will have a padlock on them, as will the drive. Depending on what policy your administrator has set, you can put data either into the encrypted container only or you can select if data shall be placed in the encrypted container or in the plaintext area of the device. The plaintext area is denoted as a folder called Unprotected Files**.** If your administrator has decided that the entire device should be encrypted, you will not see the folder called Unprotected Files.

It is possible to work with your encrypted device just like with any other removable drive in Windows, i.e. drag-drop, copy/cut-paste and all other Windows Explorer operations will work.

If a device that is already protected is inserted into a system with EEFF installed, the authentication dialog will appear automatically and after successful authentication, you will see the encrypted content as per the above description.

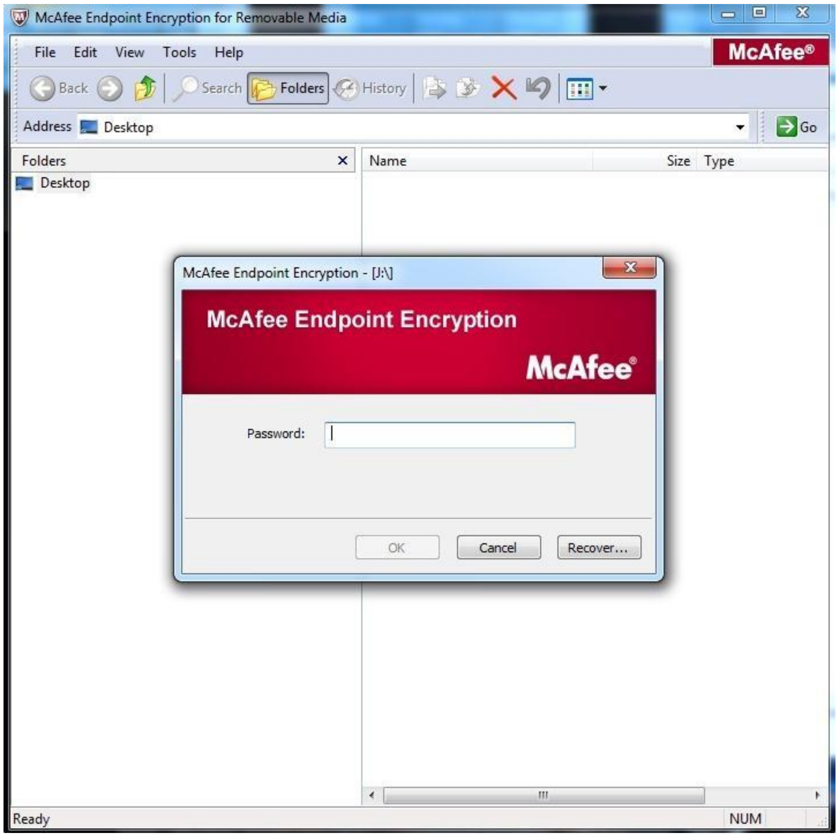
Note: Even you see a folder called Unprotected Files; your administrator may have prevented you from placing data in that folder when at work. If so, you can only read files from that folder. (This is the default setting within the NWS Endpoint Encryption System)

Working with device – "Offline"

When you insert an EERM protected device on a system without EEFF installed, e.g. your home PC, you will be presented a list of available activities for the device. One of the activities will be **Show my protected files** with the McAfee icon. If you select this activity, the EERM authentication will appear prompting you to enter valid information. You can also click **Recover…** if the password is forgotten or the certificate lost. The recovery process is described later.

If you enter a wrong password three consecutive times, the authentication dialog will offer the option to do a recovery. You may click **Yes**, in which the recovery dialog starts, or **No** in which case you will need to restart the authentication.

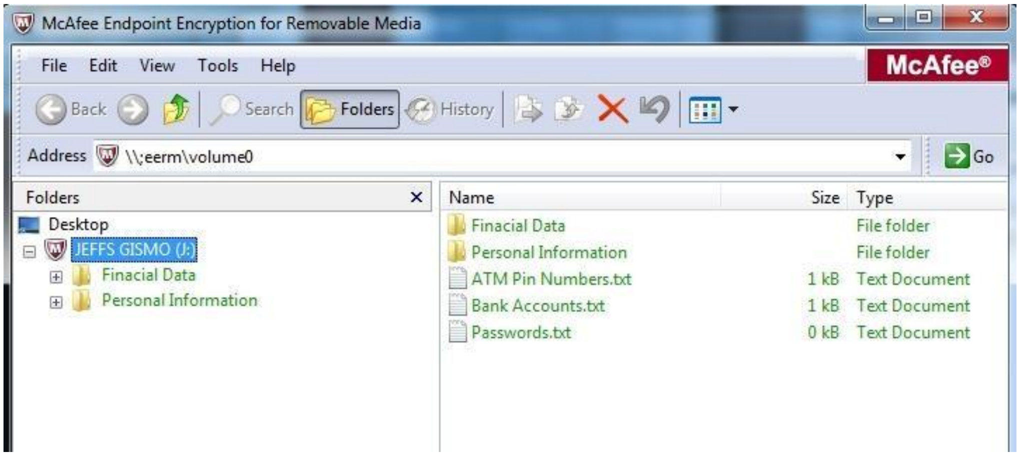
If you do not select the **Show my protected files** activity, you will need to manually start the **MFEeerm.EXE** application that resides on the root of the device in order to access the encrypted folder. This will again launch the authentication dialog.


McAfee Endpoint Encryption for Removable Media
File Edit View Tools Help
McAfee®
Back Search Folders History
Address Desktop
Go
Folders
Desktop
Name Size Type
McAfee Endpoint Encryption - [J:\]
McAfee Endpoint Encryption
McAfee®
Password:
OK Cancel Recover...
Ready
NUM

MfeEERM.exe Program Authentication

Once authenticated, you will again see the encrypted files on a drive in Windows Explorer. You can edit the protected files and save the changes to the encrypted device with retained encryption.

NOTE: If the file or folder is moved to the local system it will be moved to the system unencrypted.



Address \\;eerm\volume0

Name	Size	Type
Finacial Data		File folder
Personal Information		File folder
ATM Pin Numbers.txt	1 kB	Text Document
Bank Accounts.txt	1 kB	Text Document
Passwords.txt	0 kB	Text Document

MfeEERM.exe Program after Successful Authentication

Recovery

If you have forgotten the authentication password or lost your authentication certificate, the EERM encrypted devices can be recovered, provided you have filled in all the recovery parameters for the enabled recovery option(s).

When clicking **Recover…** in the authentication dialog, a recovery dialog will open up showing you the recovery options available.

There may be multiple recovery methods available for you, but only one can be executed (at the time). You can choose whatever recovery method you want amongst the ones displayed.

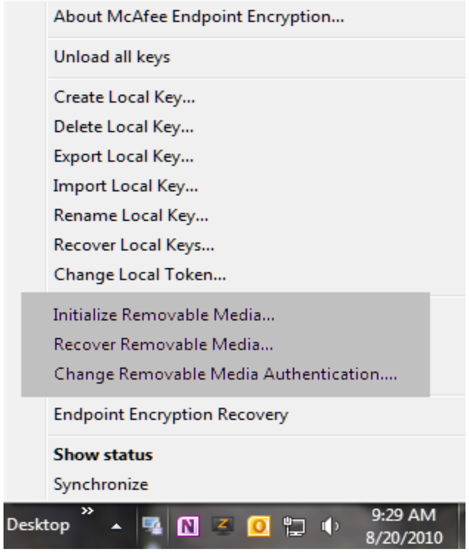
Note: With the **User Questions** recovery, it is sufficient to answer four out of five questions correct. Four correct answers will allow the recovery to succeed.

When you have entered valid recovery parameters (Challenge/response, Certificate, User questions or Recovery password), an authentication method reset dialog is presented where you are prompted to select a new authentication method, i.e. a new certificate or a new password (only one can be selected). Once selected, the recovery is complete.

“Onsite” tray icon menu

When working with EERM onsite, i.e. from a system where the EEFF client is installed, some EERM options are available on the McAfee EEFF tray icon menu.

To access the menu, right-click the McAfee EEFF tray icon located on the task bar. For EEFF, the following EERM related options are available:



EERM Tray Icon Options

Initialize Removable Media...

This option allows a manual (re-)initialization of an attached removable device. The device will be initialized as per the EERM settings in the user's EEFF policy.

Recover Removable Media...

This option launches a recovery wizard for an attached removable device protected by EERM.

Change Removable Media Authentication...

This option allows you to change the authentication token for a removable device protected by EERM, e.g. change the password or switch to certificate authentication.

Password change

To change the authentication method (change password or change certificate) when "Onsite", click the McAfee EEFF tray icon menu and select **Change Removable Media Authentication…**. This will launch a dialog where the authentication method can be changed.

To change the authentication method (change password or change certificate) when “Offsite”, from the EERM Explorer, select **Tools** from the top menu and then **Change password.** Follow the steps on the screen to complete the authentication method change.